

**XDAG : Une nouvelle crypto-monnaie basée sur le DAG**

**Introduction**

XDAG est une chaîne publique de nouvelle génération basée sur l'infrastructure du graphique acyclique dirigé (DAG), et est le premier projet DAG+POW minable et purement communautaire, avec un réseau principal lancé en janvier 2018.

L'offre maximale de XDAG est d'environ 1,446294144 milliard. XDAG n'a pas de sponsor de projet, pas d'ICO, pas de placement privé, pas de pré-minage, et est développé et maintenu par des passionnés du monde entier, ce qui est vraiment décentralisé, efficace, sécurisé et équitable.

Bien que XDAG soit un projet DAG, son modèle de transaction est similaire à l'UTXO de Bitcoin, et le développement du projet présente également certaines similitudes avec celui de Bitcoin.

**La légende de XDAG**

XDAG a été lancé en septembre 2017 par un professeur de mathématiques dans une université russe qui utilisait le nom de Cheatoshi. Parce qu'il n'était pas satifait par les projets de crypto-monnaies à cette époque, il a voulu faire un projet de crypto-monnaies de son propre chef. Il a choisi DAG et a utilisé PoW. Cheatoshin a passé trois mois à réaliser le projet mais a échoué au lancement en décembre 2017. Après que Cheatoshin ait passé quelques jours à déboguer, le réseau XDAG a démarré avec succès en janvier 2018.  
  
Le 5 janvier 2018, Cheatoshi a publié le post fondateur de XDAG sur le forum BitcoinTalk, prétendant créer un système de crypto-monnaie équitable basé sur la technologie DAG. À cette époque, tout le monde communiquait sur bitcointalk, et en février 2018, Cheatoshi a mis le projet en open-source pour que la communauté participe à la contribution, après quoi la communauté a migré le projet vers Github.   
Puis Cheatoshi a disparu et a quitté le projet a été complètement transféré à la communauté pour gérer. Cette expérience est très similaire à celle de Satoshi Nakamoto.  
Salut à Cheatoshi.  
XDAG est le premier DAG à supporter l'exploitation minière (IOTA n'est pas vraiment une exploitation minière), alors qu'il n'y a pas de pré-exploitation minière, pas d'ICO, et qu'il est entièrement géré par la communauté, sans sponsor ou investisseurs à promouvoir. XDAG est actuellement développé et maintenu en permanence par un groupe de développeurs qui aiment la blockchain et persistent dans l'idéal de la décentralisation.

**Problèmes actuels de la technologie décentralisée**

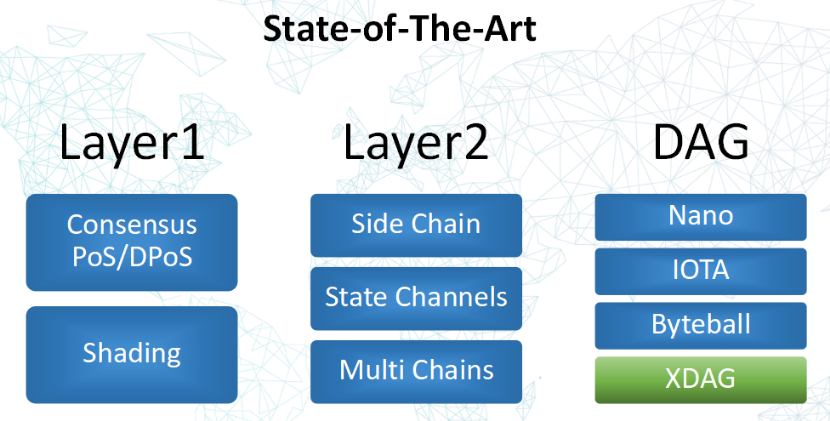
Bien que l'industrie se soit développée au fil des ans, la technologie basée sur la blockchain elle-même présente de nombreux problèmes, et ces problèmes deviennent de plus en plus graves avec l'expansion de l'échelle.

Les problèmes actuels rencontrés se situent principalement dans les deux domaines suivants.

1. Le goulot d'étranglement TPS de la blockchain elle-même limite les performances de la technologie blockchain.

2. Le long temps de confirmation de la blockchain limite également la scatibilité de la technologie blockchain.

Bien que de nombreux développeurs de blockchain dans l'industrie tentent de trouver divers moyens techniques pour résoudre ces problèmes, d'après l'état actuel du développement technique, diverses tentatives n'ont pas fait de progrès décisifs.



Les approches actuelles essayées comprennent.

**1) Couche 1 (Sharding)**

-PoS/DPoS et consensus / Sharding (calcul du sharding)

**2) Couche 2 (Side Chain)**

-Chaîne latérale/ Canaux d'état/ Chaînes multiples

Pour les défauts de la blockchain, qu'il s'agisse de la solution centralisée d'EOS ou de la technologie actuelle de sharding, il y a encore des problèmes insolubles dans la technologie de la chaîne latérale, ce qui montre indirectement qu'elle sera confrontée à de grandes difficultés et à des défis pour se développer sur la base de la blockchain elle-même. La technologie de DAG est apparue comme une troisième option de résolution.

DAG est relativement spécial, la structure des données est différente de la blockchain, et il est né avec une grande évolutivité. Le projet le plus connu utilisant la technologie DAG est IOTA, mais IOTA a toujours le problème de la centralisation ; XDAG a apporté des changements avec l'adoption de PoW, qui s'est avéré être le schéma de consensus optimal, et en laissant le travail de vérification des transactions aux mineurs exclusivement, et en conservant les avantages originaux.

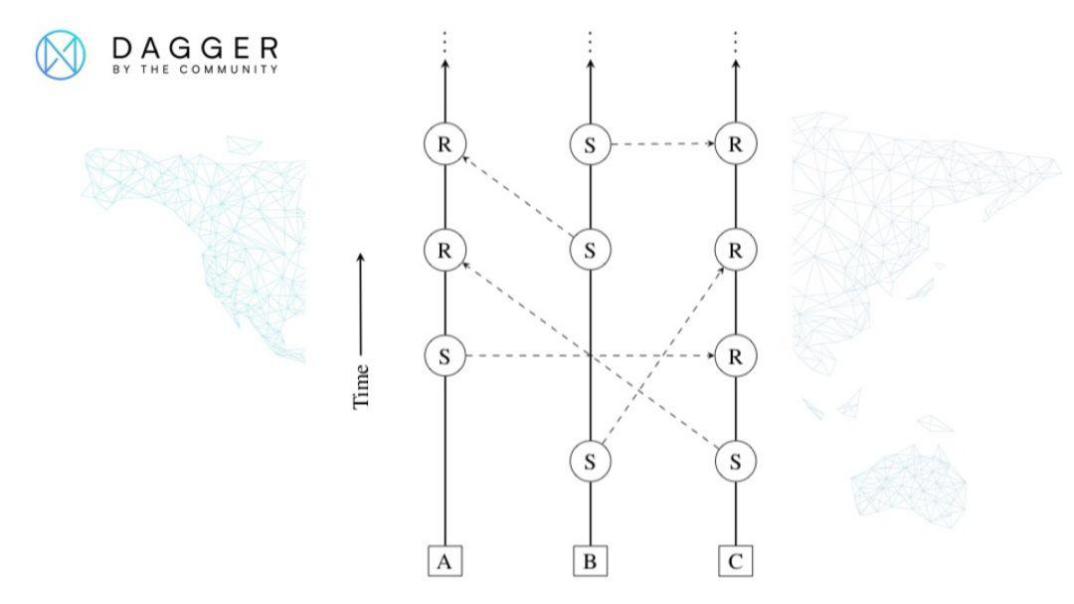
**Technologie DAG**

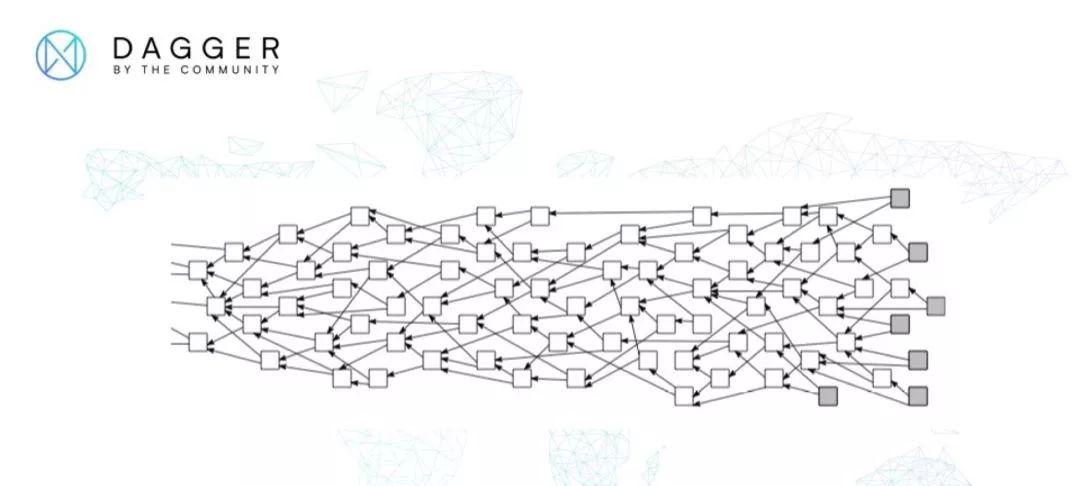
Introduit dès 1736, le DAG (**graphe orienté acyclique** ) n'est pas une technologie nouvellement apparue, mais un concept mathématique de la théorie des graphes.

En informatique, cette structure de stockage numérique existe depuis les premiers jours de la technologie. Théoriquement, les structures DAG sont plus complexes que les structures à chaîne unique, mais ont une meilleure évolutivité.

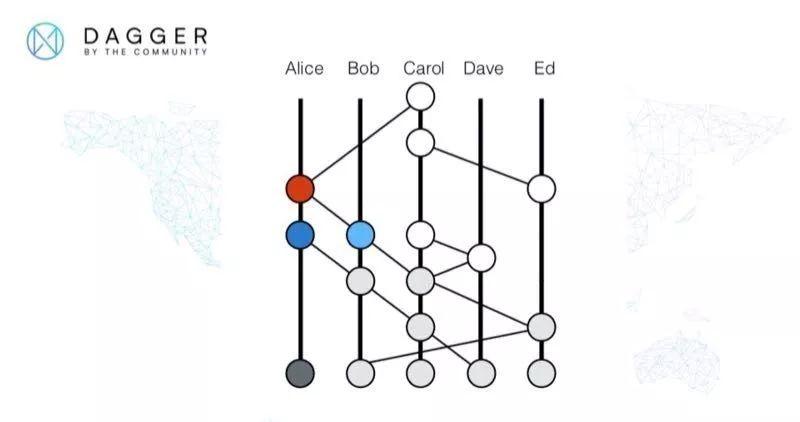
Actuellement, il y a quelques chaînes publiques basées sur la structure DAG dans l'industrie, mais chaque chaîne publique a des voies de mise en œuvre et des scénarios d'application différents en raison de la compréhension différente de la technologie DAG.

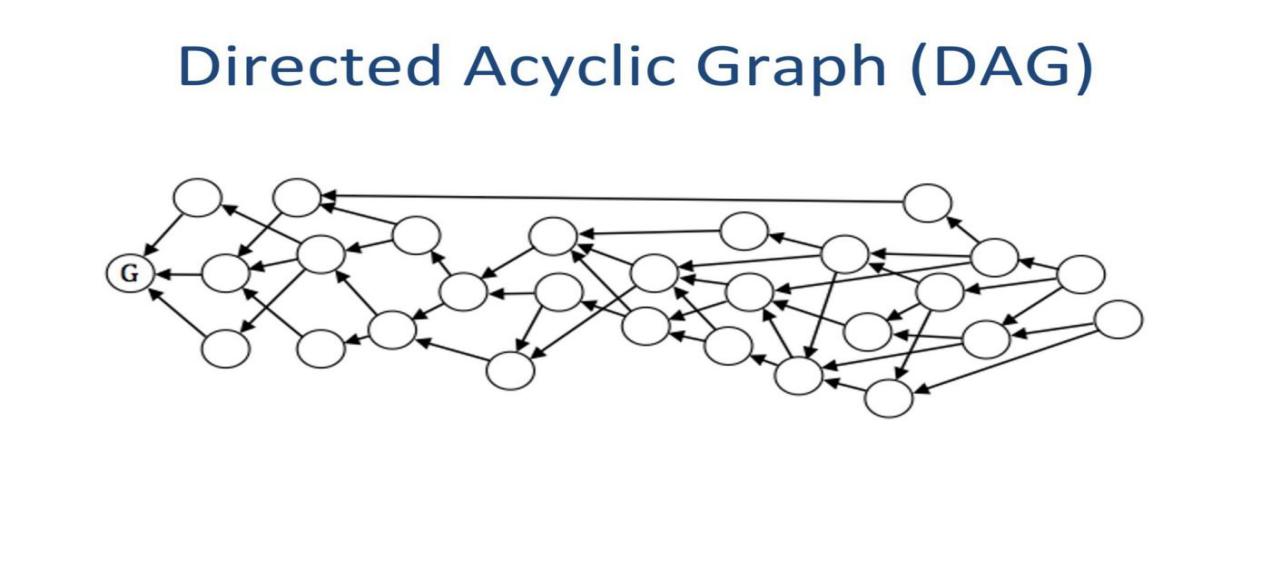
1. C'est la façon dont NANO est mis en œuvre, l'idée principale est que chaque compte a sa propre chaîne, et les différents comptes sont liés entre eux sur la base des enregistrements de transaction, formant ainsi un DAG :



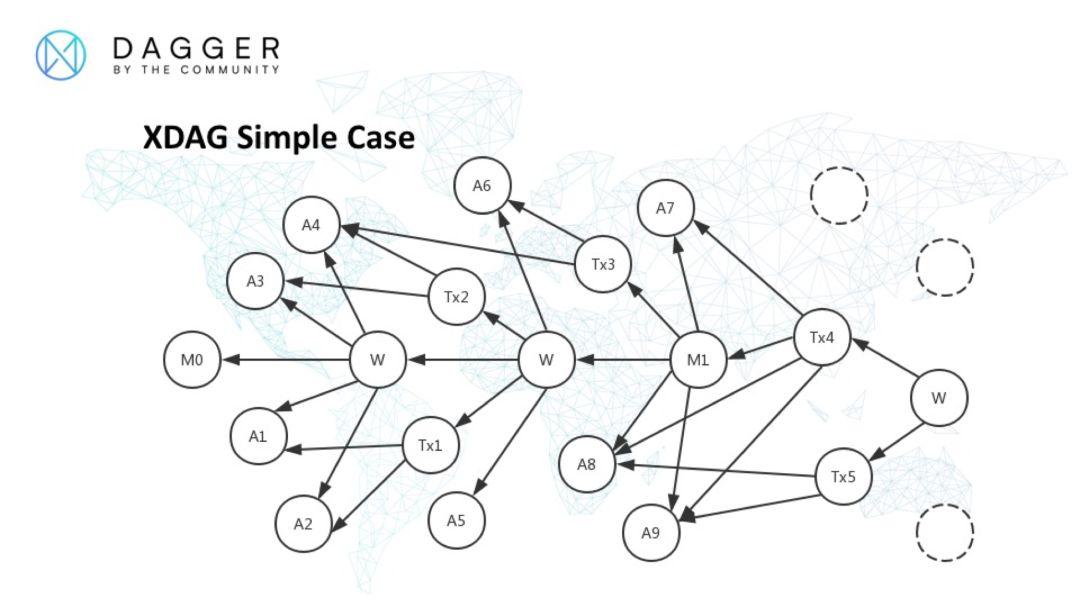
2). C'est le DAG de IOTA, et l'idée principale est de laisser l'utilisateur déterminer la validité d'une transaction en fonction de ses différentes hauteurs et poids :  
  


3). Ceci est le DAG de Hashgraph. L'idée principale est d'utiliser l'algorithme modifié de commérage entre les nœuds pour propager les informations de transaction afin de former une séquence dans le temps, formant ainsi un DAG :

  
  
4). Le DAG de Byteball, il est basé sur l'idée d'utiliser des nœuds témoins pour ajouter des unités témoins à chaque post-transaction afin d'augmenter le poids sur la branche et ainsi déterminer la chaîne maîtresse actuelle dans le DAG :



Et les implémentations de DAG multiples ci-dessus ne traitent pas le "triangle impossible", qui sont les problèmes de décentralisation, de TPS élevé et de faible temps de confirmation.  
  
XDAG tente de redessiner la structure des données à partir de la base de la technologie blockchain et adopte une autre composition DAG, combinant intelligemment l'algorithme de consensus PoW et la technologie DAG, et en même temps fournissant un traitement simultané des transactions entre les différents nœuds pour améliorer le TPS et réduire le temps de confirmation tout en assurant la sécurité et l'équité du réseau.

  
  
 Une composition partielle de DAG dans XDAG  
A = bloc d'adresse de portefeuille, Tx = bloc de transaction, M = bloc principal généré par PoW, W = bloc témoin.  
La caractéristique unique de XDAG : Blocs = Transactions = Adresses

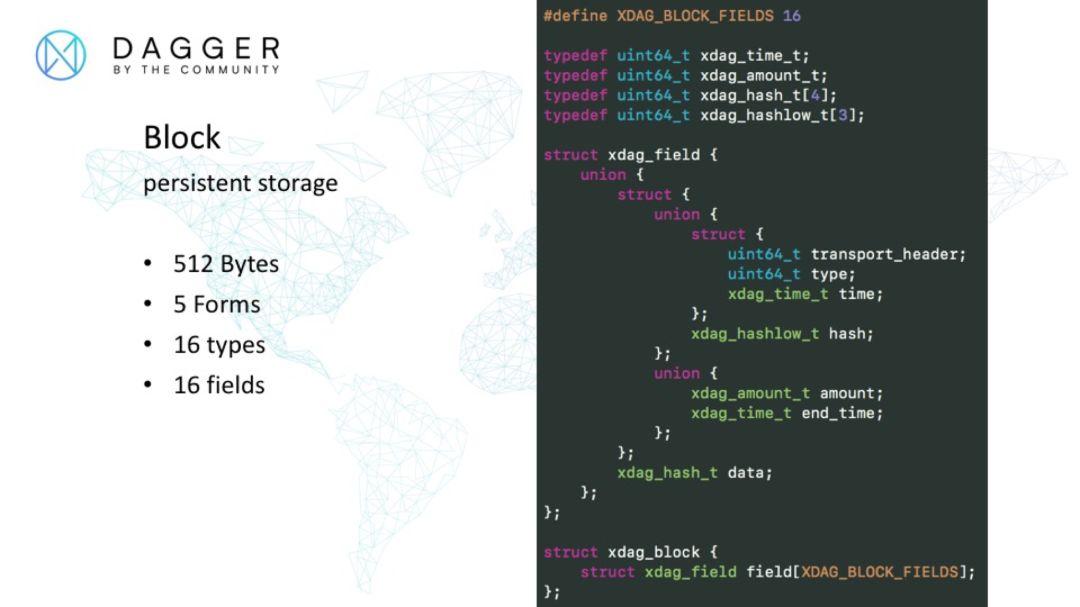
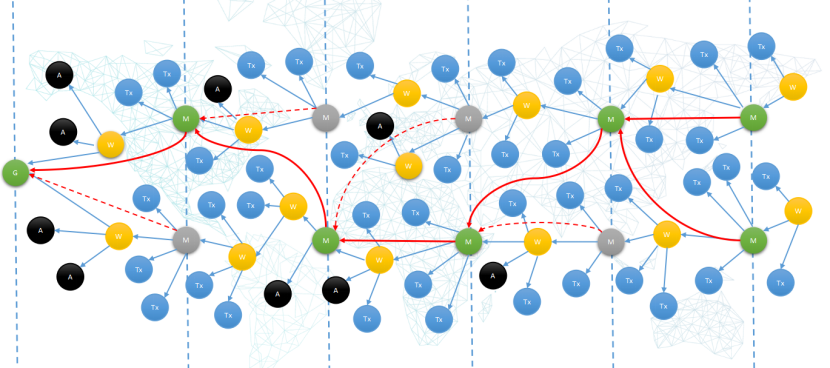
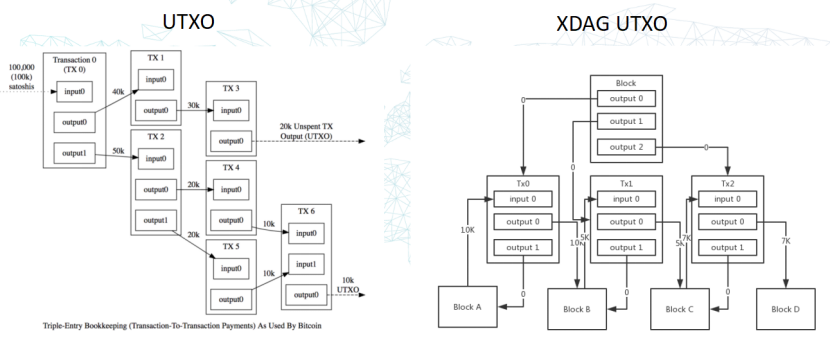
  
  
  
La structure de données du bloc dans XDAG est présentée dans la figure ci-dessus, et cette structure de données est utilisée pour le stockage persistant des données.  
  
La structure du bloc est composée de 16 structures nommées xdag\_field, chaque xdag\_field est une structure, qui consiste en une structure et une union.  
  
Le transport\_header est utilisé pour représenter le numéro de séquence pendant la transmission et pour contenir l'adresse du bloc suivant pendant le traitement post-réception.  
  
Type est un champ de 64 bits utilisé pour indiquer le type de 16 champs dans un bloc, qui est divisé en 16 parties, chaque partie est de 4 bits, c'est-à-dire un demi-octet, et 4 bits peuvent indiquer 16 types, ainsi le type de champ indique le type correspondant à un champ tous les 4 bits.  
  
Le temps est utilisé pour indiquer le temps de génération du bloc, le format utilisé est 1/1024 secondes, dans lequel une seconde est exprimée par 2^10. Il est également utilisé comme point de départ de l'intervalle de temps de la requête lorsque des données sont échangées entre les nœuds.  
  
Hash est un hachage tronqué de 24 octets, généralement le hachage tronqué d'un autre bloc.   
  
Amount est une valeur quantitative en Cheato, utilisée pour enregistrer le nombre de XDAGs, le Cheato est l'unité de base en XDAG, 1 XDAG contient 2^32 Cheato.  
  
End\_time est utilisé pour indiquer le moment de la fin de l'échange de données entre les nœuds comme plage de temps de la requête. data est un hash de 32 octets .  
  
Les blocs décrits ci-dessus dans XDAG sont générés de manière totalement indépendante par chaque Node et chaque portefeuille lui-même sans interférence des autres, assurant ainsi l'indépendance du traitement des blocs dans la conception de base, et posant les bases du TPS élevé mentionné par la suite.  
  
**3. Avantage technologique de XDAG.**  
  
1) XDAG est la première chaîne publique basée sur DAG à réaliser le PoW. En combinant la haute concurrence de DAG avec la sécurité et la décentralisation de PoW pour résoudre le problème du "triangle impossible" dans la technologie blockchain ;  
2) Bloc = Transaction = Adresse.  
Cette conception unique garantit que le processus de transfert ne perdra pas de pièces en raison de la saisie d'une mauvaise adresse ;  
3) Faibles frais de transaction et TPS élevé.  
4) XDAG utilise une technologie unique pour résoudre de nombreux problèmes qui peuvent exister dans le système de blockchain, tels que la double dépense, le temps de transaction incontrôlable, la centralisation, les attaques à 34% et à 51%.  
5) Certaines des expériences actuellement réalisées sur le Bitcoin et l'Ether peuvent être réalisées sur XDAG, car les fondateurs ont réalisé leurs propres systèmes d'exploitation, ils ont donc été conçus dans cette optique.  
  
Celles-ci peuvent être expliquées comme les figures ci-dessous :

Diagramme 1 :

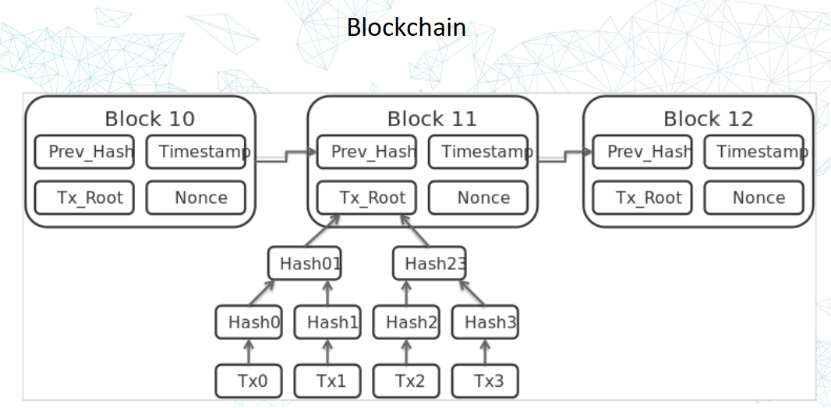


Il y a un concept de chaîne principale dans DAG, parce que les transactions dans DAG ont besoin d'un tri, sinon il ne peut pas résoudre le problème de double-dépense. XDAG à l'intérieur de la chaîne principale, il y a une tranche selon le temps, chaque tranche sera emballée pour les transactions, Vert est le bloc principal sur la chaîne principale, Jaune est le bloc témoin, Bleu est la transaction de transfert, Noir est le bloc adresse.

Diagramme 2 :

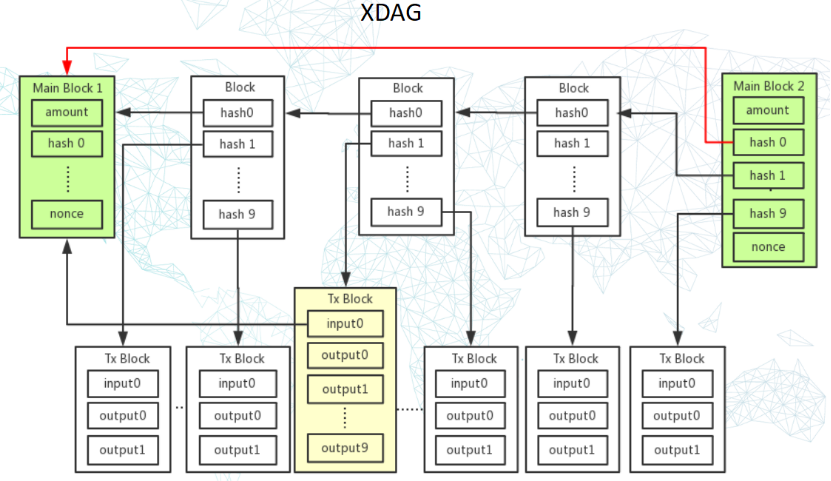


XDAG est similaire à Bitcoin et est également le modèle d'UTXO. Les graphiques ne sont peut-être pas les mêmes, mais l'essence est la même, le bloc dans la figure est le bloc de connexion mentionné plus tôt, Tx0, Tx1, Tx2 sont les transactions réelles, et les blocs A - D sont les adresses.  
  
  
Diagramme 3 :



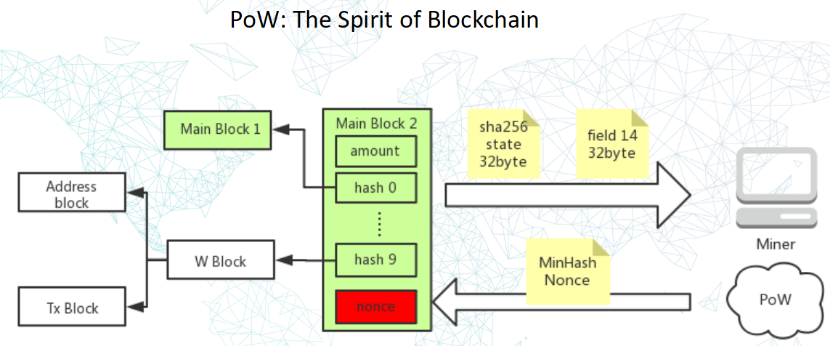
D'après la figure ci-dessus, il y a des arbres de Merkle dans la blockchain et une structure similaire dans XDAG.

Diagramme 4 :



Le bloc principal vert dans la figure ci-dessus stocke le hachage de la transaction, similaire à l'arbre de Merkle.  
  
Le calcul du PoW dans XDAG est variable, les mineurs ajoutent les transactions reçues à leur propre calcul de hachage, chaque nœud fera le calcul, et finalement rivaliser qui a la plus forte puissance de calcul, et ensuite générer le bloc de la chaîne principale.

Diagramme 5 :

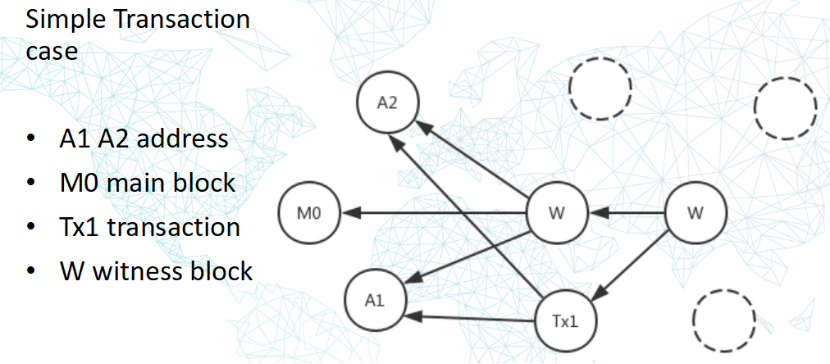


Il s'agit de faire le hachage que le calcul du bloc local / transaction, couche par couche, et enfin remplir le nouveau bloc (bloc principal 2), et ensuite faire le calcul sha256, ce que sha256 fait est de faire le calcul itératif et l'obscurcissement. Pour l'envoi du résultat, seule la valeur sha256 calculée doit être envoyée au lieu d'envoyer toutes les transactions, la taille est seulement de 32byte, ce qui permettra d'économiser les ressources de la bande passante, de sorte que le mineur a seulement besoin de continuer à calculer le sha256 et enfin trouver un hachage minimum pour obtenir le nonce et déterminer le nouveau bloc principal sur la chaîne principale, et de cette façon la structure de la chaîne principale est formée.  
Note : Pour assurer l'équité, l'algorithme minier XDAG a été changé de sha256 à l'algorithme RandomX.

1. **Comment résoudre le problème de la double dépense ?**

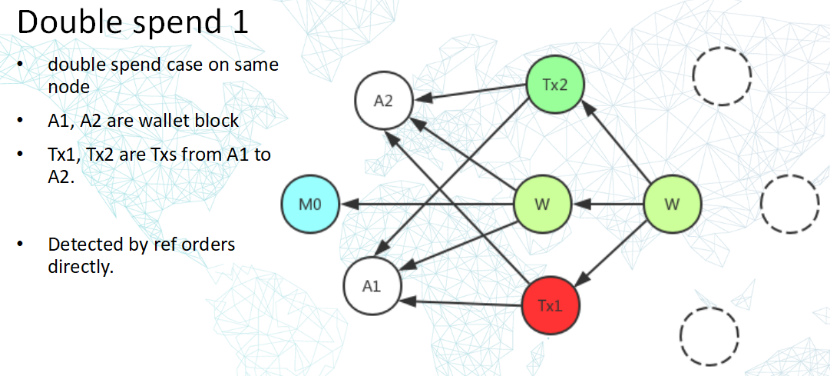
Ceci peut être illustré par les diagrammes ci-dessous :

**Diagramme 1 :**

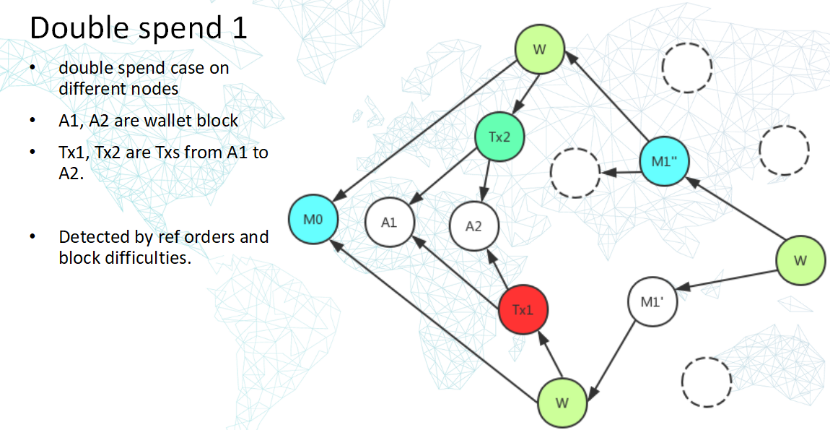


Si une transaction est générée entre A1 et A2, un nouveau bloc de connexion est généré pour confirmer la transaction entre eux, et le bloc de connexion est généré par les mineurs.

**Diagramme 2 : Une détection typique de double dépense**



Supposons qu'il y ait 10 XDAG à l'adresse A1, que le portefeuille de A1 soit malicieusement copié deux fois et que deux transferts soient initiés en même temps, un Tx1 transfère 5 XDAG de A1 à l'adresse A2, et l'autre Tx2 transfère 7 XDAG de A1 à l'adresse A2. Les deux transferts totalisent 12 XDAGs, ce qui dépasse les 10 XDAGs originaux pour l'adresse A1, une double dépense typique.  
La logique dans la détection des XDAGs est que lorsque le nœud reçoit Tx1 et Tx2 en même temps, le nœud génère un bloc W qui fait référence à Tx1 et Tx2, et selon les règles d'ordonnancement stable, Tx2 sera peuplé de champs avec des numéros d'ordre plus petits lorsqu'ils sont référencés par le bloc W, ainsi Tx2 est traité en premier et Tx1 est traité plus tard, vérifiant ainsi que la dépense Tx1 est une double dépense, et ainsi le bloc interne sera Le bloc de transaction pointé par ce hachage est marqué comme rejeté, et le bloc de transaction Tx1 est enregistré dans le DAG pour toujours et n'est pas supprimé.  
Étant donné que les utilisateurs peuvent choisir à quel nœud envoyer leurs transactions pour vérification, on suppose ici que si les deux transactions sont envoyées au même nœud, la première transaction référencée par le bloc de connexion est une transaction valide, et la seconde est une transaction non valide, résolvant ainsi le problème simple de double dépense.  
  
  
**Diagramme 3 : Une détection plus complexe de la double dépense**



Supposons que la prémisse est la même que la précédente, et supposons qu'il y ait 10 XDAG à l'adresse A1, et que le portefeuille de A1 soit malicieusement copié deux fois et que deux transferts soient initiés en même temps, un Tx1 transfère 5 XDAG de A1 à l'adresse A2, et l'autre Tx2 transfère 7 XDAG de A1 à l'adresse A2. Les deux transferts totalisent 12 XDAGs, dépassant les 10 XDAGs initiaux à l'adresse A1, une double dépense typique.  
Mais cette fois, la situation a changé, c'est-à-dire que la personne a malencontreusement utilisé des moyens techniques pour connecter le portefeuille à un nœud différent, créant ainsi une détection de double dépense entre des nœuds différents.  
  
À ce stade, le consensus PoW entre en jeu, et un bloc maître est généré toutes les 64 secondes dans XDAG. En comparant la difficulté du bloc maître M1' M1'', il est déterminé que M1'' est plus difficile, donc M1'' référence le bloc Tx2 en priorité de tri par rapport à M1' référence Tx1, de sorte que Tx1 est détecté comme une fleur double, et donc le bloc de transaction pointé par ce hash est marqué comme rejeté dans le bloc interne, tandis que le bloc de transaction Tx1 est enregistré dans le DAG pour toujours et ne sera pas supprimé.

S'il y a un utilisateur qui veut tricher et envoie ces deux transactions à des nœuds différents, cette fois il est nécessaire de résoudre ce problème par le bloc maître généré par PoW (M1''), comme vous pouvez le voir sur la figure ci-dessus M1'' est le bloc maître généré par la compétition arithmétique PoW des mineurs, tandis que M1' ne l'est pas, parce que le bloc maître a la priorité, dans ce cas, Tx2, qui est indirectement référencé par M1'', est une transaction valide résolvant ainsi le problème de Double Spend.

**5. XDAG supporte un TPS élevé.**

Pourquoi le XDAG permet-il d'atteindre un TPS élevé ? C'est parce qu'il divise le DAG en plusieurs blocs localisés, ce qui permet d'atteindre un TPS élevé similaire à l'effet du calcul de sharding.

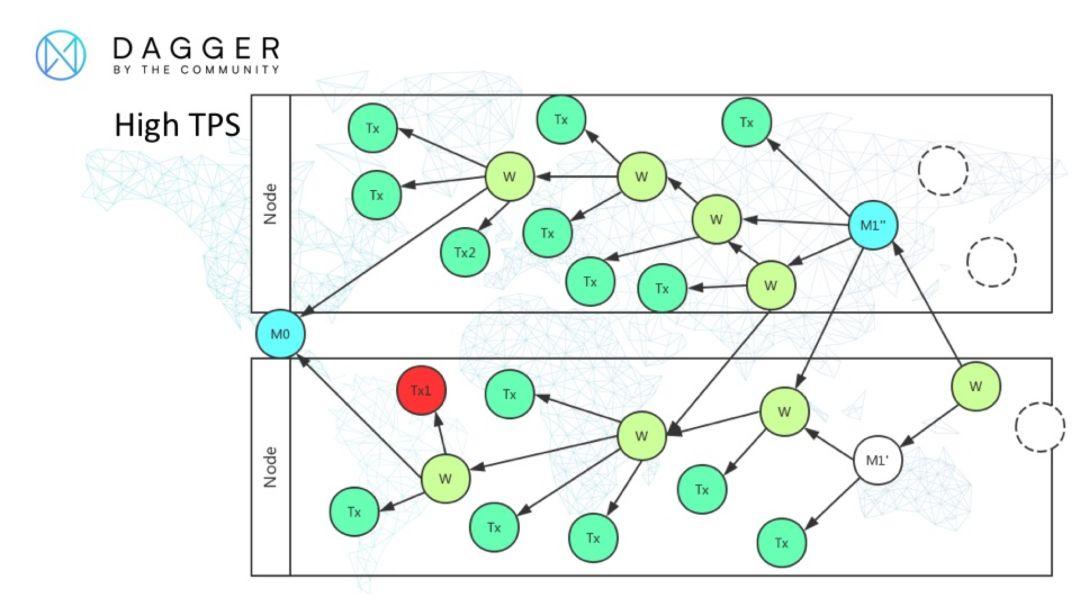


Diagramme 1 :

Le diagramme montre une structure DAG plus complète de XDAG, où les blocs d'adresses de porte-monnaie dans les diagrammes précédents sont omis pour plus de simplicité.

Node désigne un nœud différent, M désigne le bloc principal extrait par PoW, W désigne un bloc supplémentaire, que j'ai nommé bloc témoin, et Tx est le bloc de transaction.

Les différents nœuds reçoivent leurs propres blocs de transaction séparément, et l'acte d'assemblage des blocs de transaction dans le DAG est moins couplé les uns aux autres, et la connexion entre eux est établie par l'interaction des données entre les nœuds, ce qui permet aux différents nœuds d'absorber une plus grande concurrence bien pour atteindre un TPS élevé.

Dans le même temps, un bloc maître est généré toutes les 64 secondes par PoW, de sorte que le temps de confirmation des transactions des chaînes publiques décentralisées est également considérablement réduit, et peut être confirmé en 1 à 2 minutes en général.

**Avantage de XDAG**

1. XDAG adopte la méthode DAG + PoW pour briser et résoudre les limites de la technologie blockchain traditionnelle, ce qui peut améliorer considérablement l'évolutivité du système blockchain. XDAG a les avantages de la décentralisation et d'un TPS élevé tout en supportant l'exploitation minière PoW. Le réseau XDAG peut encore avoir un TPS élevé sous la décentralisation la plus originale comme le consensus PoW, et le volume de transaction peut atteindre plusieurs milliers de TPS.

Théoriquement, l'approche DAG est qu'il peut y avoir un nombre illimité de blocs de transaction entre les blocs principaux, mais la situation réelle dépend toujours de la vitesse de transmission du réseau et de la performance des équipements sur le réseau. Le volume de transaction de pointe a déjà atteint plusieurs milliers de TPS, cependant, en raison des conditions du réseau et du matériel, la limite de transaction n'a pas été mesurée.

2. Un bloc dans XDAG est également une transaction, et l'adresse générée par le portefeuille générera également une transaction dans le réseau : Bloc = Transaction = Adresse. Certaines des expériences actuellement réalisées sur le Bitcoin et l'ETH peuvent être réalisées sur XDAG, car les fondateurs eux-mêmes ont réalisé le système d'exploitation, ils en ont donc tenu compte dans la conception.

3. Génération rapide de blocs, transfert rapide et pas de commission. Grâce aux caractéristiques de la technologie DAG de l'infrastructure, XDAG est actuellement réglé pour générer un bloc toutes les 64 secondes, le transfert peut être d'environ 3 minutes sur le compte, la commission est nulle. Ceci est dans le cas de la décentralisation PoW, pour atteindre un TPS élevé et un transfert rapide.

4. XDAG peut atteindre la sécurité financière, sans adresse de trou noir. Toutes les adresses de portefeuille et les enregistrements de transaction dans XDAG sont des blocs, tant qu'il y a un portefeuille, alors l'adresse du portefeuille doit exister dans le réseau principal ; si vous essayez de transférer de l'argent à une adresse inexistante échouera, il n'y a donc pas de problème de transfert à une adresse de trou noir.

5. Originalité de XDAG. L'implantation de DAG+PoW dans XDAG est révolutionnaire et la plus ancienne (Note : vérifiez l'heure à travers le post Genesis de BitcoinTalk), et le code est original. XDAG fournit le langage C et Java.

6. Totalement géré par la communauté. Pas de sponsor de projet, pas de pré-minage, pas d' ICO, chaque XDAG est miné et extrait par les mineurs. L'équipe de la communauté est composée de passionnés de différents pays, qui ensemble conduisent l'évolution de XDAG.

7. Résistance aux ASIC et minage des CPU. XDAG adopte l'algorithme minier RandomX pour attirer plus d'utilisateurs de CPU à rejoindre le minage, plus d'équité.

Avec ces avantages, XDAG peut supporter de nombreuses applications de scénario décentralisé, permettant à plus d'applications d'être portées sur XDAG, sans la douleur de la congestion et des frais élevés des autres chaînes publiques.

**Communauté XDAG**   
  
Les enthousiastes de XDAG ont mis en place une équipe autonome de la communauté, du développement libre de geek à l'avancement ordonné, du programme Apollo au programme Mars actuel, XDAG fait des progrès rapides une étape à la fois et la communauté devient de plus en plus forte.  
  
Actuellement, l'équipe autonome de la communauté XDAG est composée de plus de 20 membres du monde entier, dédié à XDAG JAVA/C , portefeuille PC, portefeuille Android, portefeuille IOS, algorithme minier, logiciel minier, protocoles de réseau, site web communautaire, testnet, opérations communautaires et autres travaux différents.  
La charge de travail est encore relativement importante pour une communauté autonome, nous avons besoin de plus de passionnés de XDAG pour nous aider.

Actuellement, la communauté a mis en place un mécanisme de proposition communautaire (https://trello.com/b/nlSBXa2d/xps) et un mécanisme d'incitation des développeurs, que vous trouverez a cette adresse : <https://xdag.io/task>

Tout le monde peut suggérer des améliorations sur XPS et sponsoriser les coûts de développement.

Liens XDAG  
Site officiel： xdag.io  
Bitcointalk：https://bitcointalk.org/index.php?topic=2552368.0  
XDAG Whitepaper：https://github.com/XDagger/xdag/blob/master/WhitePaper.md  
Github：https://github.com/XDagger  
Blockchain Explorer：https://explorer.xdag.io/  
Exchanges： coinex.com   
Bienvenue dans la communauté XDAG  
Discord：https://discord.gg/Nf72gd9  
Télégram：https://t.me/dagger\_cryptocurrency  
Twitter：https://twitter.com/XDAG\_Community  
Wechat：xdag\_dev